(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 May 2001 (17.05.2001)

PCT

(10) International Publication Number
WO 01/35685 A1

(51) International Patent Classification[7]: H04Q 7/32, H04L 9/32

(21) International Application Number: PCT/DK00/00620

(22) International Filing Date:
9 November 2000 (09.11.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PA 1999 01608 9 November 1999 (09.11.1999) DK

(71) Applicant *(for all designated States except US)*: **MOBILIX A/S** [DK/DK]; Prags Boulevard 80, DK-2300 Copenhagen S (DK).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **WARD, Christian, Paul** [GB/FR]; Résidence Le Clos Royal, Bât. B, 80, rue Alfred Duméril, F-31400 Toulouse (FR).

(74) Agent: **CHAS. HUDE A/S**; H.C. Andersens Boulevard 33, DK-1780 Copenhagen V (DK).

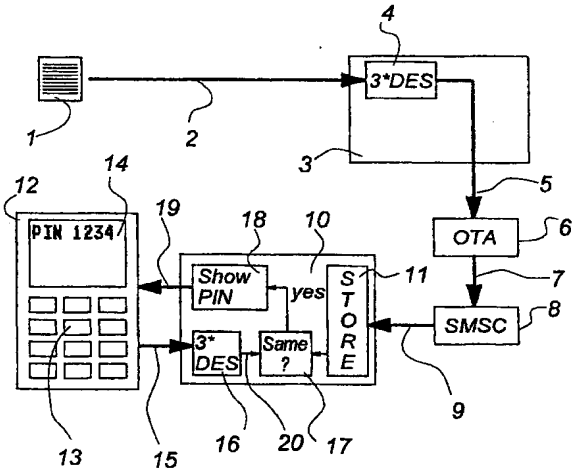
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*
— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM FOR ELECTRONIC DELIVERY OF A PERSONAL IDENTIFICATION CODE



(57) Abstract: A system is provided for electronic delivery of a PIN code in a secure, fast and efficient manner and compromising a server (3) provided with a reference code (2) for generating the PIN code. The server (3) is adapted to transmit a SMS message (9) containing an electronic signature (5) based on the reference code (2) to a SIM card (10) connected to a terminal (12). The SIM card (10) comprises means (11) for receiving and storing the SMS message (9), and means (17) for comparing the stored electronic signature (5) in the SMS message (9) with an electronic signature (20) generated from a reference code (15) entered by a user of the terminal (12). Encryption keys, generated by a triple DES data encryption algorithm having two keys, and encryption means are provided in the server (3) and in the SIM card (10).

WO 01/35685 A1

System for electronic delivery of a personal identification code.

Technical Field

The invention relates to a system for electronic delivery of a PIN (Personal Identification Number) code and comprising a server secured by means of a number of encryption keys and provided with a reference code for generating the PIN code, said system further comprising means for encrypting the reference code and the PIN code generated by means of the encryption keys and via connected communications means being adapted to transmit a SMS (Short Message Service) message containing an electronic signature based on the reference code to a SIM (Subscriber Identity Module) card connected to a terminal with input and display means.

Background Art

Personal identification numbers, so-called PIN codes, are presently used in many different situations, in particular in connection with economic transactions, in which a credit card or a similar means of payment is used together with a terminal. The information stored on the credit card is verified by the card user during completion of the transaction by entering a PIN code on the terminal's keyboard, said code being agreed with the card issuer. It is thus ensured that the user of the card is identical to the owner of the card.

The PIN code is usually assigned to the credit card in connection with the issuance thereof and generally forwarded to the user under separate cover as ordinary mail. This method is neither completely secure nor very fast, as it may take several days for the letter to reach the card owner and thus before the owner can use his card.

Brief Description of the Invention

The object of the invention is to provide a secure, fast and efficient system which is able to deliver PIN codes to the customers in a more advantageous manner.

A system of the above type is according to the invention characterised in that the SIM card comprises means for receiving and storing the encrypted SMS message, means for comparing the stored electronic signature based on the reference code in the SMS message with a reference code entered by a user of the terminal, said reference code subsequently being used to generate an electronic signature by means of a corresponding encryption key in the SIM card, and means for allowing subsequent display of the PIN code associated with the signatures on the display means of the terminal, if the stored and the entered electronic signatures match. It is thus only possible to be advised of a given PIN code, if the user of a specific terminal enters the associated reference code. The exchange of the PIN code and the reference code is made exclusively in form of encrypted data signals which can only be decrypted by using the two unique encryption keys. A high degree of security delivery of PIN codes is thus obtained.

Furthermore according to the invention the electronic signature in the secure server and the electronic signature in the SIM card may be generated by a data encryption algorithm (triple DES algorithm) having two keys, each key having a word length of at least 56 bit. Such an encryption algorithm provides a high decree of security against unauthorised decryption attempts.

Moreover according to the invention the communications means connected to the secure server may use a radio communications link for transmitting the SMS message to the SIM card connected to the terminal. It is thus possible to use a mobile handset to receive SMS messages.

Furthermore according to the invention the reference codes may comprise at least six alphanumeric digits, whereby the reference code may for instance be civil

registration numbers, account numbers, names, key words and any other information only known to the user.

Finally according to the invention the electronic signature based on the reference code may be transmitted to the SIM card in encrypted form at the same time as the SIM card is provided with a unique identification number. As a result, unauthorised decryption of PIN codes during transmission thereof are prevented and the security of the system is thus enhanced.

Brief Description of the Drawing

The invention is explained in greater detail below with reference to the accompanying drawing illustrating a flow chart of a preferred embodiment of the invention.

Best Mode for Carrying Out the Invention

The system for electronic delivery of a PIN code shown in the drawing comprises a secure server 3 adapted to receive unique information 1 (illustrated as a chart for filling-in personal data) in form of reference codes 2, and encryption means 4 subsequently computing the electronic signature 5 based on the reference code 2 in the server 3. The server 3 communicates with a so-called over-the-air platform 6 (OTA) communicating with a SMS service centre 8 adapted to receive encrypted information 7 from the platform 6. The SMS service centre 8 is connected to a SIM card 10 which communicates with a mobile GSM handset 12 comprising a keyboard 13 and a display means in form of a display 14, said service centre being able to transmit completed SMS messages to the SIM card 10. The SIM card 10 comprises a storage 11 for storing encrypted SMS messages 9, encryption means 16 for encrypting data 15 entered by a user of the terminal 12 via the keyboard 13 and comparator means 17 connected to the storage 11 and the keyboard 13 for comparing the stored data with entered data. The comparator means 17 are further connected to

means 18 for displaying the PIN code on the display 14 of the terminal 12.

When using the system the user delivers unique information 1 in form of a reference code 2 to the secure server 3. The reference code 2 is used as an input signal for generating an electronic signature 5 in the server 3 by means of the encryption means 4. The electronic signature 5 is transmitted via the over-the-air platform 6 to the SMS service centre 8 for administration of the SIM card, said service centre 8 converting the electronic signature 5 to a SMS message 9 suitable for transmission thereof to the SIM card 10 in question connected to the mobile handset 12. The SIM card 10 comprises a storage 11 adapted to receive and store the encrypted SMS message 9. The comparator means 17 are used for comparing the electronic signature 5 in the encrypted SMS message 9 with the electronic signature 20 generated by the encryption means 16, said signature 20 being generated on the basis of data entered on the keyboard in the terminal 12. If the electronic signature 5 and the electronic signature 20 entered by the user match, the comparator means 17 transmits a signal to the guide means 18 that the PIN code 19 is to be displayed on the display 14 of the mobile handset 12, whereby the PIN code is delivered to the user.

In a preferred embodiment of the invention the terminal 12 is a mobile handset such as a cellular telephone. A SIM card (Subscriber Identity Module) is required for operating mobile handsets adapted for communication via an existing GSM network. The SIM card, which in use forms an integrated part of the electronics of the mobile handset, contains *inter alia* codes identifying the mobile handset in relation to the GSM network. This identification is necessary to enable the network to determine for instance the position of the mobile terminal for transmission of mobile telephony via the most advantageous transmission tower(s) in the network at the specific time.

The server 3 comprises software (not shown) for generating PIN codes, a triple DES (Data Encryption Standard) encryption algorithm (reference numeral 4), an encrypted database (not shown) containing encryption keys to all of the SIM cards registered

in the system and information about the connection between the numbers of the mobile handsets and the numbers of the associated SIM cards. A triple DES algorithm is a three-level encryption process which is considered particularly secure against unauthorised decryption.

When the secure server 3 has received the reference code from a new user and verified that the user's SIM card number is valid in the system, the server 3 generates an electronic signature 5 preferably by means of the triple DES algorithm 4 combined with the two at least 56 bit keys belonging to the user's SIM card number. The electronic signature 5 is transmitted to the user's SIM card 10 as uniquely formatted GSM 8 bit SMS (Short Message System) messages. The coding of the SMS messages is adapted such that the electronic signature 5 of the reference code 2 is stored in the storage 11 of the SIM card 10 and the user is notified that the generated PIN code is ready for use when a SMS message 9 is received by the user's SIM card 10.

When the user subsequently runs the program in the SIM card 10 enabling delivery of the PIN code, the user is requested by the program via the display 14 of the terminal to enter the reference code 15 on the keyboard 13 of the terminal 12. For generating another electronic signature 20, the reference code 15 is coded by the encryption means 16 in the SIM card 10 by means of the same encryption algorithm used by the encryption means 4 in the secure server 3 when the reference code 2 was supplied to the secure server 3. The comparator means 17 in the SIM card 10 then compares the electronic signature 5 stored in the storage 11 and based on the reference code 2 with the electronic signature 20 generated by the encryption means 16. If the two signatures match, the comparator means 17 transmits a signal to the control means 18 indicating that the PIN code 19 is to be displayed on the display 14 of the terminal 12. If the two electronic signatures are not identical, the user is advised on the display 14 that the reference code 15 has not been accepted and is asked to enter the reference code 15 once more. If the reference code 15 after two

additional attempts still is incorrect, the program is terminated and the PIN code 19 is not delivered until the user has fetched a new reference code 2 from the secure server 3, said code being either identical to or different from the initial reference code 2.

In order to ensure that the delivered PIN code is read correctly, the user may be offered to validate the delivered PIN code. The validation process is performed by the user entering the PIN code shown on the display 14 by means of the keyboard, whereafter the user is advised whether the PIN code has been entered correctly. If not, the PIN code is shown once more on the display 14 and the validation process is repeated.

In an alternative embodiment the PIN code may be provided in the SIM card, when supplying the card with a unique identity code, whereby the PIN code never need be transmitted. This is considered a more secure embodiment preventing unauthorised decryption of the PIN code during transmission thereof.

The invention is not restricted to the above preferred embodiment, but may be altered in many ways without thereby deviating from the scope of the invention.

Claims

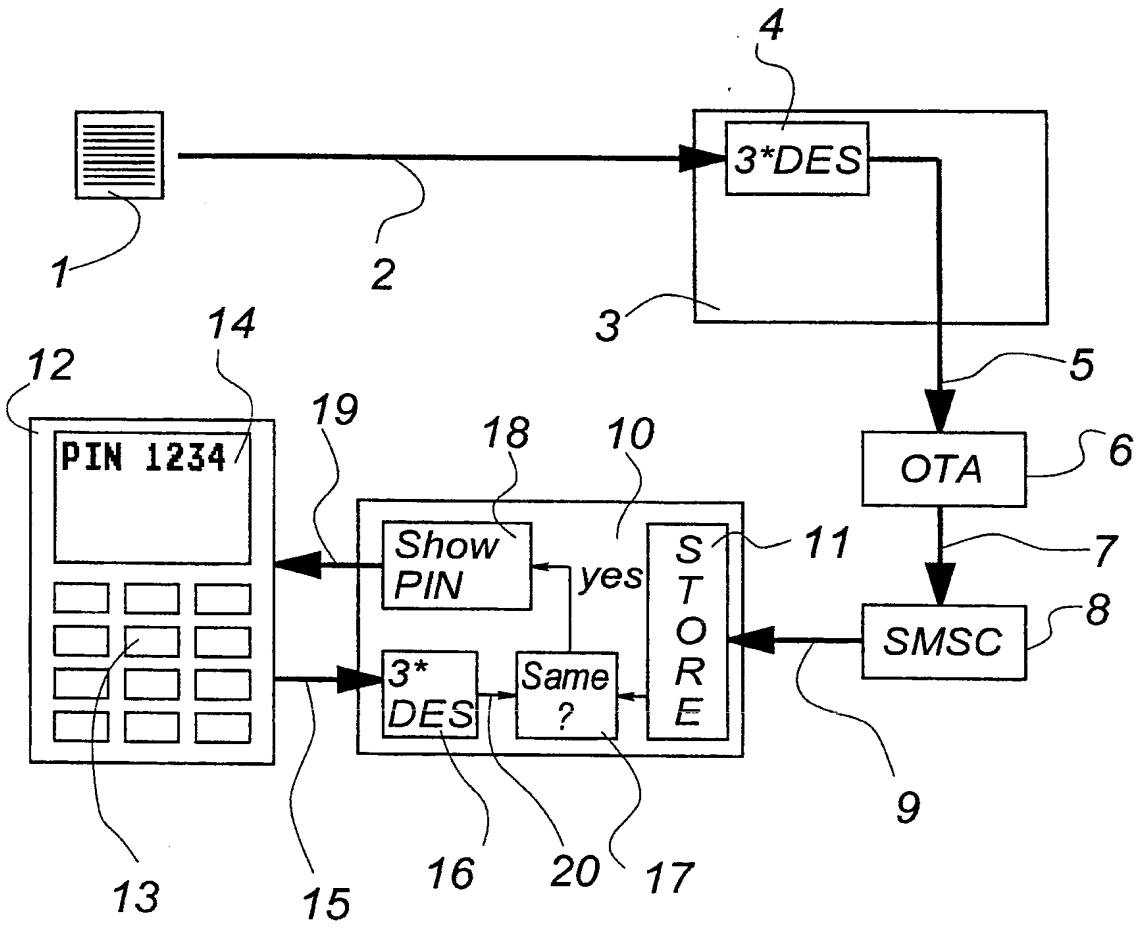
1. A system for electronic delivery of a PIN (Personal Identification Number) code and comprising a server (3) secured by means of a number of encryption keys and provided with a reference code (2) for generating the PIN code, said system further comprising means (4) for encrypting the reference code and the PIN code generated by means of the encryption keys and via connected communications means (6,8) being adapted to transmit a SMS message (9) containing an electronic signature (5) based on the reference code (2) to a SIM card (10) connected to a terminal (12) with input means (13) and display means (14), c h a r a c t e r i s e d in that the SIM card (10) comprises means (11) for receiving and storing the encrypted SMS message (9), means (17) for comparing the stored electronic signature (5) based on the reference code (2) in the SMS message (9) with a reference code (15) entered by a user of the terminal (12), said reference code (15) subsequently being used to generate an electronic signature (20) by means of a corresponding encryption key (16) in the SIM card (10), and means (18) for allowing subsequent display of the PIN code associated with the signatures (5,20) on the display means (14) of the terminal (12), if the stored signature (5) and the entered electronic signature (20) match.

2. System according to claim 1, c h a r a c t e r i s e d in that the electronic signature (5) in the secure server (3) and the electronic signature (20) in the SIM card (10) both are generated by a data encryption algorithm (triple DES algorithm) having two keys, each key having a word length of at least 56 bit.

3. System according to claim 1 or 2, c h a r a c t e r i s e d in that the communications means (6, 8) connected to the secure server (3) uses a radio communications link for transmitting the SMS message (9) to the SIM card (10) communicating with the terminal (12).

4. System according to one or more of the preceding claims, characterised in that reference codes (2, 15) comprise at least six alphanumeric digits.

5. System according to one or more of the preceding claims, characterised in that the electronic signature (5) based on the reference code (2) is transmitted to the SIM card (10) in encrypted form at the same time as the SIM card (10) is allocated an unique identification number.


4
3*DES
1
2
3
5
14
12
19
18
10
PIN 1234
OTA
6
Show PIN
yes
S T O R E
11
7
3* DES
Same ?
SMSC
8
9
13
15
16
20
17